DOCUMENT RESUME

ED 129 929 TM 005 808

AUTHOR Stephens, Kent G.
TITLE A Fault Tree Approach to Needs Assessment -- An Overview.
PUB DATE Apr 76
NOTE 21p.; Paper submitted to the Needs Assessment Conference (Oakland, California, April 8, 1976)

EDRS PRICE MF-$0.83 HC-$1.67 Plus Postage.
DESCRIPTORS Educational Technology; Failure Factors; Logic; *Methods; *Needs Assessment; Success Factors
IDENTIFIERS *Fault Tree Analysis

ABSTRACT

A "failsafe" technology is presented based on a new unified theory of needs assessment. Basically the paper discusses fault tree analysis as a technique for enhancing the probability of success in any system by analyzing the most likely modes of failure that could occur and then suggesting high priority avoidance strategies for those failure modes. It provides a logical, step by step approach to the identification of possible failure factors and the interactive effects of those factors which could result in a predetermined undesired event. The fault tree is so named because the completed graphic portrayal of logic gate related potential failure sequences takes on the outline form of a branching tree. (Author/RC)

A FAULT TREE APPROACH TO NEEDS ASSESSMENT--AN OVERVIEW

By

Kent G. Stephens, Ph. D.

A Paper

Submitted to the

Needs Assessment Conference

April 8, 1976

Oakland, California - Edgewater Hyatt

A FAULT TREE APPROACH TO NEEDS ASSESSMENT

AN OVERVIEW

Recent events are continuing to signal concern by the public over the question of who is going to guard the guards. This concern is also evidence of a continuing loss of license by educators to manipulate the public and their students. In some instances this is causing some educational leaders to question the survivability of such trends as competency and performance based educational programs. For example, one can ask "whose competency and performance standards? And, more importantly, why?" Answers to this question should provide some visibility of who and where the manipulators are or at least provide some warning of the potential for Theory X assumptions to emerge in these endeavors.

In any event it is clearly evident that the educator will find himself in a future with reduced opportunity to directly manipulate the public and students. This paper proposes a technology as part of a general unified theory of educational needs assessment based on the concept of *educational stewardship* which will be defined as *the responsibility of each educator to make it* ***safe*** *for others (including organizations) to find their own best way.* Emphasis is placed on "safe" in order to find a place for accountability since the unaccountable person or organization does not appear to be very safe according to the demands of contemporary society.

However, a dilemma is posed by this definition. Suppose a child is about to place his hand on a hot stove. The dilemma revolves around the question of should the steward withhold the hand of the child in the name of safety or let the child find his own best way and learn by burn?

Traditional attempts to balance a trade off between freedom and safety have produced such manipulative schemes (some more subtle and intellectually legitimatized than others) as competency and performance based educational programs, management by objectives, behavioral objectives, instructional objectives, etc. What is needed is a method of balancing freedom and safety in a less manipulative way.

If a unified approach to educational need's assessment can be suggested by the previous definition of educational stewardship, then a theoretical framework by which needs assessment can be developed in a less manipulative manner providing a reasonable balance between freedom and safety of educational endeavors is also suggested.

Three basic approaches to this framework are presented as needs assessment activities in lieu of the more traditional methods which have led to CBTE, PBTE, etc. These are:

1. Identify and make visible opportunities for people and/or their programs.

2. Identify and make visible potential hazards to people and/or their programs.

3. Legitimazation of hazards and opportunities which have been illuminated.

The first activity listed above is not treated in this paper.

The second activity is the approach which is discussed in the rest of this paper under the general heading of Fault Tree Analysis. The third activity will be treated only in terms of a process for legitimazation of hazards once identified.

There are two basic approaches to analysis: (1) analysis in terms of success or accomplishment of system's purpose, or (2) analysis in terms of failure or non-accomplishment of a system's purpose.

Analysis in terms of success, however, is much more problematic than analysis in terms of failure. Not only is it difficult to achieve consensus as to those design characteristics and functions, the channels and interactions, which lead to system success, but experience has shown that in complex systems, it is much easier to describe and achieve consensus as to what constitutes failure. When a system is functioning smoothly, it is not at all easy to specify precisely what combinations of events contribute to this state. But when breakdowns occur, they are immediately apparent, although their causes and their "downstream" effects may be more obscure.

Fault Tree Analysis (FTA) is a technique for enhancing the probability of <u>success</u> in any system by analyzing the most likely modes of <u>failure</u> that could occur and suggesting high priority avoidance strategies for those failure modes. It provides a logical, step by step description of possible failure events within a system and their interactions--that is, the combinations of potential occurrences which could result in a predetermined undesired event (U.E.). The fault tree was so named because the completed graphic portrayal of a functional system utilizes a branching process.

It is not the intent of this paper to present a detailed explanation of the technique of performing a Fault Tree Analysis. Explanations of both qualitative and quantitative analysis, examples of educational and management information applications, and prototype trees may be found in Stephens (1972).

Description of Fault Tree Analysis

Following is a brief overview of the steps in Fault Tree Analysis. It should be noted that the fault tree approach can be used in a more simplified,

abbreviated form, and still be very useful. In fact, implementers have found that they could derive useful information from any of the steps followed in performing a fault tree analysis.

Qualitative Fault Tree Development

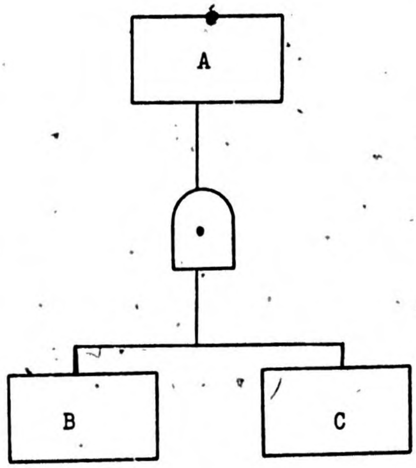
A fault tree consists of events, interrelated by logic gates, which are formed into sequences of potential failures. The analysis begins with the precise statement of an undesired event (UE) of critical importance. It may be the failure of the entire system, expressed as a failure of the mission; or it may be a failure identified with some subsystem or component. In any event, it stands at the top of the tree, and the analysis proceeds downward. Inputs to the UE become contributing failure events in a perceived cause and effect relationship.

Before discussing the nature of the events, however, it is necessary to clarify the concept of logic gates. The heart of the fault tree approach, and that which differentiates it from other forms of analysis, is the use of logic gates to show the relationships among events. There are two principal kinds of logic gates, the AND gate and the OR gate. All other gates used are derivatives of these two.

The AND logic gate is used when two or more events must coexist in order to produce the more general event. The AND gate is symbolized graphically by the symbol . In the fault tree, events related by an AND gate would be depicted as in Figure 1.

Figure 1

THE AND GATE



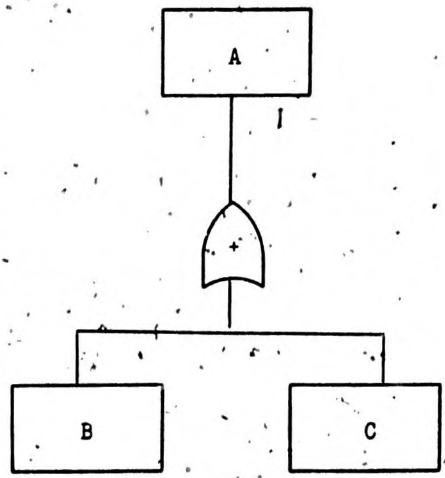
This would be read: Events B and C must coexist to produce Event A; or, the output can occur only if the inputs B and C coexist. The mathematical equivalent of this is $A = (B \wedge C)$.

In behavioral systems, this relationship most commonly exists when a subsystem or component and one or more backup systems or components exist or are possible within the design of the system. This situation occurs much less frequently in behavioral than in hardware systems, and the implications of this will be considered later in this paper in regard to the interpretation of the tree.

The OR logic gate is used when, of two or more possible inputs to an event, any one alone could produce the output. The graphic symbol for the OR gate is  . In the fault tree, events related by an OR gate would be depicted as in Figure 2.

Figure 2

THE OR GATE



This is to read: Either B or C alone will produce Event A. The mathematical equivalent of this is A = (B $\vee$ C).

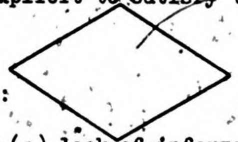
There are two general kinds of OR gates--the INCLUSIVE OR and the EXCLUSIVE OR. In the INCLUSIVE OR situation, either B or C or both could result in Event A. In the EXCLUSIVE OR situation, either A or B could produce C, but both A and B could not occur simultaneously.

With either the AND or OR gates, more than two inputs may exist. Variations of these gates allow for the specification of complex relationships--there are inhibit gates, priority AND gates which specify the sequence of events, matrix gates, and others. The analysis thus provides precise description of conditions as well as modes of relationships, all of which can be expressed mathematically and quantified.

The other set of basic symbols used in fault tree analysis depicts the types of inputs or events. Input and output events can be classified according to their nature. The following are the most commonly used symbols for fault trees:

Rectangle:  Identifies an event that results from a combination of less general fault events through an associated logic gate. All events symbolized by rectangles have additional development in the fault tree.

Circle:  Identifies a basic failure event that requires no further development. This could occur when the definition of an event is sufficiently explicit to satisfy the purpose of the analysis.

Rhombus:  Identifies an event which is not developed further due to (a) lack of information, (b) very remote likelihood of occurrence, or (c) because time, financial or other constraints preclude further analysis.

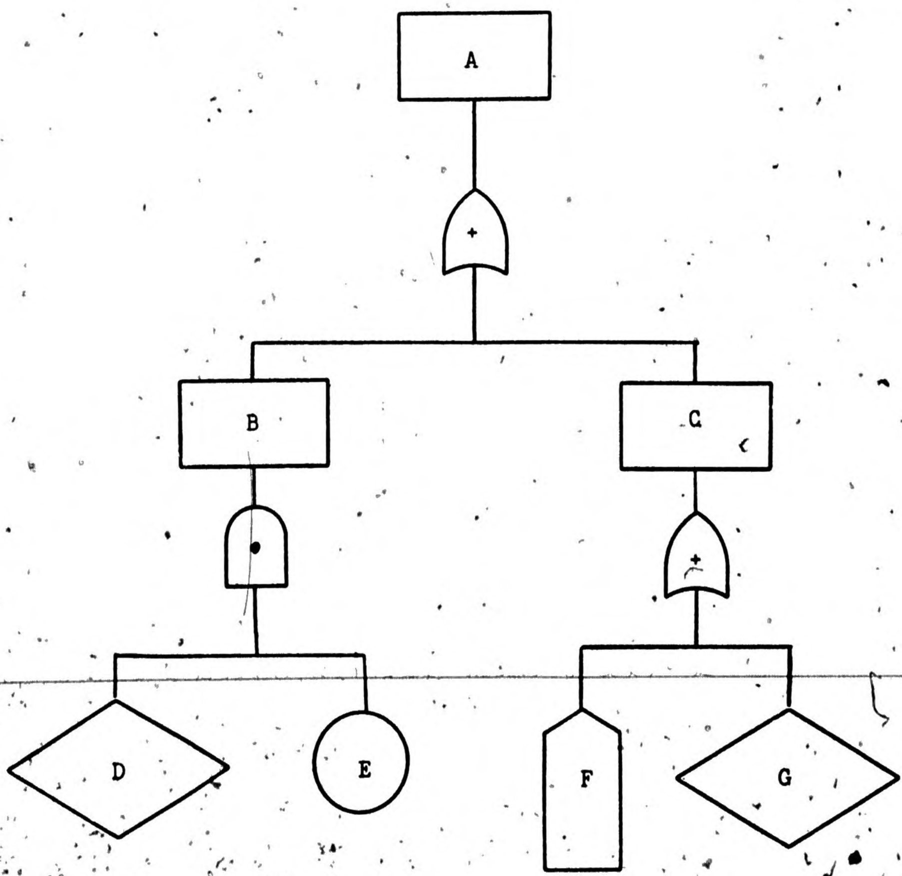
House:  Identifies an event that is normally expected to occur in the system as defined. When combined with other events, however, it might contribute to a failure event.

Figure 3 shows a rudimentary fault tree, which is read as follows: "Event A can be produced <u>either</u> by Event B <u>or</u> Event C or both. Event B can be produced only by the coexistence of Events D <u>and</u> E. Event C can be produced either by Event F or Event G or both." Event E is a primary or basic failure event, and Event F is an event that normally occurs in the system, but which can contribute to Event C. Events D and G are not analyzed further in in this tree due to reasons beyond the current scope of analysis of the tree.

The "bottom of the tree" for any branch always will have events depicted by the circle, rhombus, or house. In this example, there are two branches and three levels of analysis.

Figure 3

ILLUSTRATION OF A FAULT TREE BRANCH



For each given event, which in turn becomes a UE, failure events contributing to more general undesired events can be derived according to several models. One approach is to systematically ask questions regarding input, processing, output, and environmental factors; i.e., failures of a given component or subsystem may be attributable to failures of input from another part of the system, failures of processing within the component or subsystem itself, failures of output to another part of the system, or failures attributable to an abnormal environment.

Figure 4 can be used to illustrate how failure analysis can be applied to a system which operates serially, Events A, B, and C being prerequisite conditions to Event D. In 4a the events are assumed to be operating successfully; i.e., for success of D, a single thread of events is necessary from A to B to C to D. In 4b the events are graphically analyzed for potential failure; that is, failure of D can be caused by failure of either A or B or C or any combination of them.

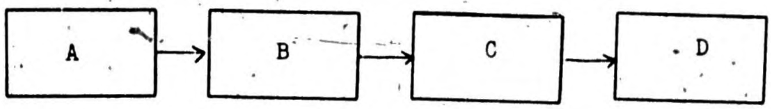
Figure 5 shows another possible system configuration, using both concurrent and prerequisite conditions for success. Diagram 5a assumes the system to be operating successfully. For success of D, the flow of events or information must go from A to B then to C_1 or C_2 before D can occur. Diagram 5B shows the events as analyzed for potential failure. Failure of D can be caused only by failure of C_1 and C_2 failing concurrently. C_1 can be caused by the failure of A or B or both; C_2 can also be caused by the failure of A or B or both.

Another point to note is that it appears from Figures 4 and 5 that analysis for failure is simply the logical reciprocal of analysis for success. To an extent this is true, in that experience has shown that reduction of the likelihood of an undesired event from occurring can be accomplished through

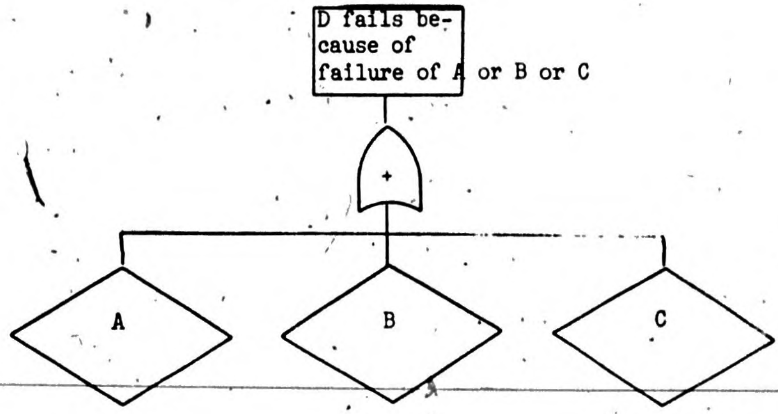
Figure 4

COMPARISON OF ANALYSIS IN SUCCESS SPACE WITH ANALYSIS IN FAILURE SPACE FOR PREREQUISITE EVENTS IN A SERIES

(a) system design



(b) failure analysis of above system design in terms of the failure of event D



(c) success analysis of system design in terms of the success of event D

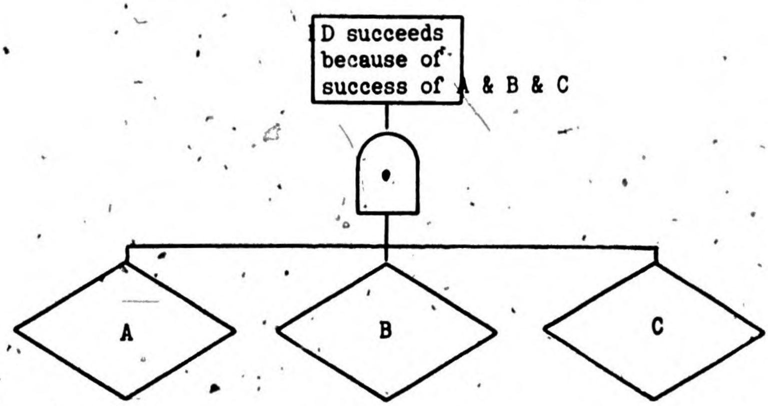
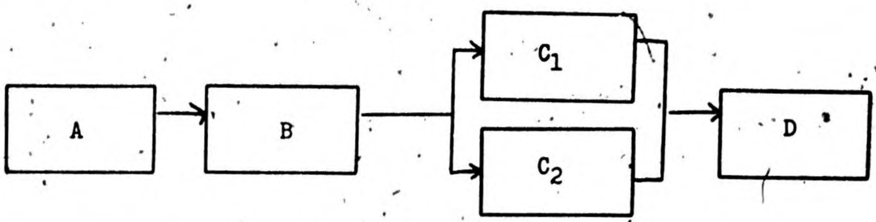


Figure 5

COMPARISON OF ANALYSIS IN SUCCESS SPACE WITH ANALYSIS IN FAILURE SPACE FOR CONCURRENT AND PREREQUISITE EVENTS

(a) system design



(b) failure analysis of above system design in terms of the failure of event D

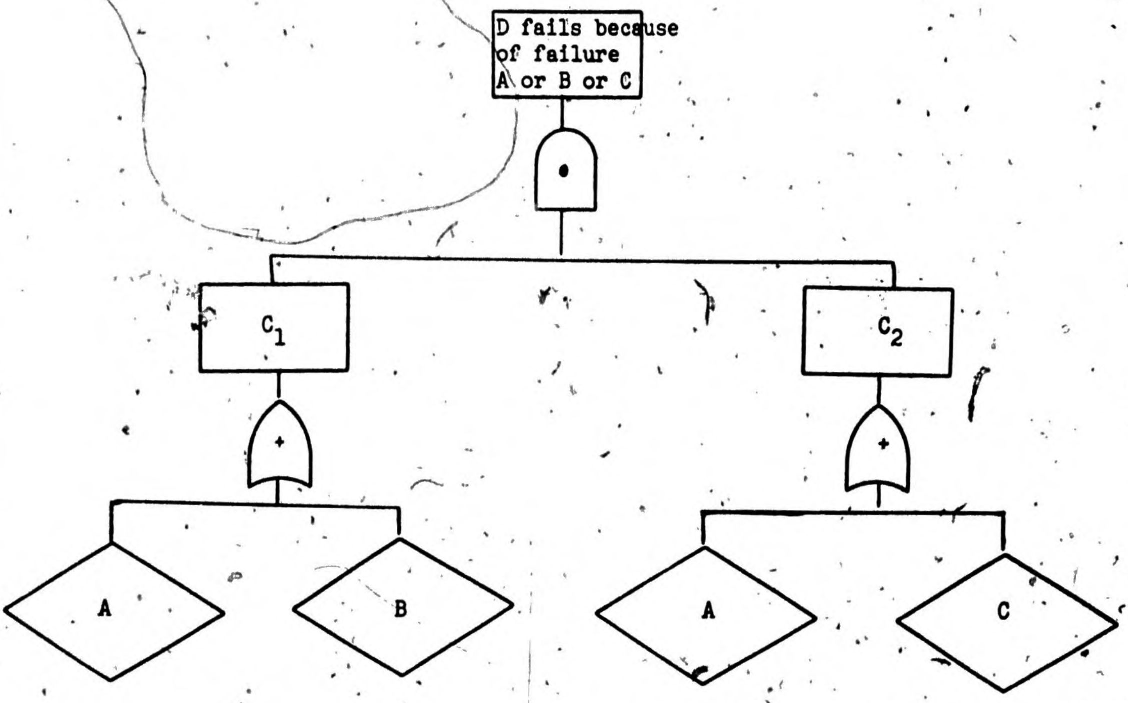
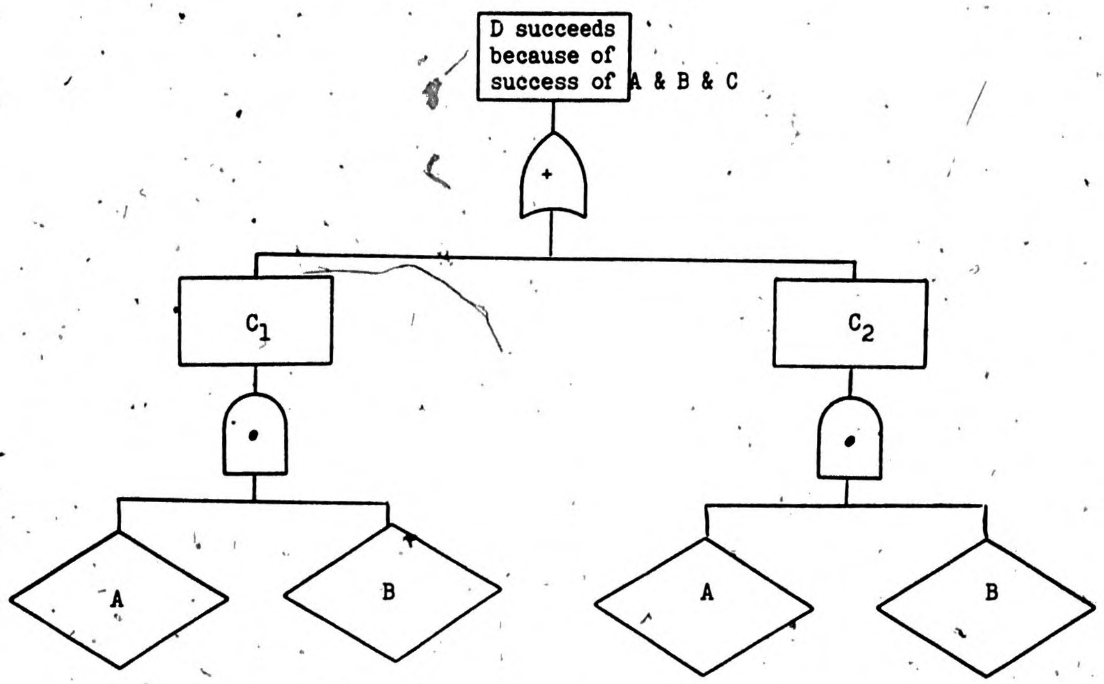


Figure 5
continued

(c) success analysis of system design in terms
of the success of event D



changing or monitoring the sequences of events on the primary strategic paths determined on a fault tree.

Recent work with FTA of complex systems, however, has shown that failure analysis gives perspectives on a system which go beyond the simple logical inversion of success analysis to failure analysis and back again. In fact, the FTA methodology itself appears to have a heuristic value, both for those participating in the analysis and the managers and other decision makers to whom the results and recommendations are communicated. It generates questions about the system which do not occur under the usual conditions of success analysis. Additionally, the methodology, by facilitating consensus formation

processes of groups, promotes team building activities which, in turn, lead to greater productivity.

Quantitative Fault Tree Development

Derive one or more strategic paths through quantitative Fault Tree Analysis (FTA)

Quantitative Fault Tree Analysis utilizes four basic judgements as follows:

(1) Starting with the top UE, rank in order of relative contribution (or importance) each of the failure events leading into it.

For all of the inputs through a given logic gate to a single more general event, determine the percentage contribution made by each event to the more general failure event above it. Percentages should sum up to 100 for each event.

(2) Determine confidence in the percentages (strong, moderate, and weak are commonly used).

Repeat the above steps for the inputs to each failure event, working systematically down through the tree.

(3) Determine the appropriate frequency rating for each event at the bottom or lowest level only for each branch of the tree (rarely, periodically, and frequently occurring are commonly used). That rating for each input to an event is determined independently of the other inputs for that same event.

(4) Determine the rectification for each event (permanent damage or impossible to rectify, difficult to rectify, and easy to rectify are commonly used). These judgments are combined through formulas derived from Markov Processes and Boolean Algebra to yield strategic event values in order to identify strategic paths of interest by inspection.

Although a computer program is available for deriving strategic paths (as well as for drawing the tree), the computations can be done by hand. On

trees of more than 300-350 inputs, however, the hand process is too time consuming. Even without completing the quantification, however, much valuable information regarding the operation of the system can be gained by simple inspection of the tree.

It is not necessary for most of the team members engaged in qualitatively constructing the tree or quantifying it to know more than the rudiments of fault tree principles. The main requisite is a good working knowledge of the system under analysis. Team members should represent many different levels and functions within the organization, as the various "levels of visibility" afforded by different personnel will lead to perspectives differing in important respects. These perspectives are dealt with directly in the quantification process. Experience has shown that wide divergences of opinion can be recondiled without being ignored or subdued. Furthermore, the technique accommodates and utilizes both "hard" data and expert opinion.

The final step in FTA is to make recommendations based upon the strategic path analysis. These may include reallocating resources, installing backup systems, providing for monitoring of paths with high failure potential, redesigning sybsystems, or taking any other corrective action that seems advisable. Displaying the fault tree and discussing the strategic paths and their implications with personnel at various levels of the organization often will bring excellent suggestions for improvement and an increase in cooperative effort to work toward organizational goals, and is an excellent non-threatening approach to giving visibility to needs that have been identified.

History and Background of FTA

FTA is an operations research technique in which one form has been used with signal success as a major analytical tool of system safety engineering

in the hardware industry. Rudimentary concepts of FTA originally were developed by Bell Telephone Laboratories as a technique for performing a safety evaluation of the Minutemen Launch Control System. Bell engineers discovered that the method used to describe the flow of "correct" logic indata processing equipment could also be used for analyzing the "false" logic resulting from component failures. (Haasl, 1965) The format was also well suited to the application of probability theory in order to define numerically the critical fault modes.

Additional development of the analytical and mathematical techniques of Fault Tree Analysis in hardware systems occurred in the Boeing Company. For further descriptions of the history and development, see Ericson (1970) and Stephens (1972).

Since 1967, however, the author has successfully applied FTA to a number of educational, managerial, and research problems.

An important breakthrough for FTA of non-hardware systems came with the development (Stephens, 1972) of a new quantification scheme for deriving strategic paths through the use of subjective probabilities. The viability of strategic path analysis for management decisions in educational systems has been repeatedly demonstrated through the author's analysis of the various educational systems and problems.

The FTA method used for generating inputs, tends to focus the thinking of the group on specifics and to organize all inputs within a systematic framework. Moreover, experience with very different kinds of fault trees (e.g., vocational education, research project management, community college needs assessment) has shown that the technique has other advantages in a multi-disciplinary team effort.

1. It focuses expert knowledge and judgment from often widely disparate disciplines and functions on a common problem and furnishes a common language and perspective.

2. It can take into account both agreements and divergences on the inputs and their importance.

3. It allows for concentration on one area of interest at a time, but with the assurance that all other areas will be systematically dealt with.

4. By concentrating on the way the system operates, rather than on personalities, it introduces a non-threatening atmosphere and encourages a freer exchange of information among the members.

A serendipitous effect of FTA on participating members of an organization has been noticed. Without exception, those who have actively participated in working with the analyst to derive inputs for the qualitative and quantitative analysis have gained a new perspective of the system and have turned from somewhat passive members to active workers for system success.

Any approach to analysis must deal with the complexities and interdependencies which are an inherent part of any behavioral system. A characteristic of systems is that stress in any part of the system will eventually make itself felt in other parts, perhaps far removed from the stress point itself. It often happens, however, that a problem, such as a breakdown in communication, is perceived as having its source in one part of the system when, in fact, its "real" causes are elsewhere.

FTA is capable of dealing with such secondary effects of stress in the system, of spotting and analyzing redundant failure events which may have significant cumulative impact, and of defining interactions among events which appear to be unrelated. The quantification process adds power to the qualitative analysis in accomplishing this.

To sum up. FTA has been found useful as the principle analytic method for conducting a needs assessment under at least the following conditions:

1) Whenever undesired events or concerns and factors contributing to those concerns can be identified;

2) Whenever differing areas of expertise must be marshalled;

3) Whenever involvement of the members of an organization needs structure and systematizing;

4) Whenever a defensible approach to resource allocation within a complex system is needed;

5) Whenever consensus as to what constitutes success in the system is difficult to obtain;

6) Whenever formative evaluation is necessary;

7) Whenever the primary <u>and</u> secondary effects of future decisions must be analyzed.

It is hoped that more educators will consider analysis for failure as well as analysis for success in educational needs assessment.

REFERENCES

Archibald, Russel D. and Richard L. Villoria. Network-Based Management Systems. PERT/CPM. New York: John Wiley & Sons, Inc., 1968.

Burhans, David T., Jr. The Development and Field Testing of Two Internal Communication Measuring Instruments. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Butler, Katharine G. Competency Programming in Special Education. First Progress Report. California State University at San Jose, Department of Special Education. October 15, 1972.

Campbell, Robert M. and Hutchin, David. The Delphi Technique: Implementation in the Corporate Environment. Management Services, No.-Dec., 1968, pp. 37-42.

Campbell, Vincent N. and David G. Markle. Identifying and Formulating Educational Problems. A report to the Far West Laboratory for Educational Research. Palo Alto, California: American Institute for Research, Dec. 1967.

Cooper, Bernice. An Analysis of the Behaviors of Principals as Observed and Reported in Six Critical Incident Studies. Journal of Educational Research, 56:8, 1963, pp. 410-14.

Driessen, Gerald J. Cause Tree Analysis: Measuring How Accidents Happen and the Probabilities of Their Causes. Paper presented at the 78th Annual Convention of the American Psychological Association, Miami Beach, Florida, Sept. 3-8, 1970.

Ericson, C. System Safety Analytical Technology--Fault Tree Analysis, 1970. The Boeing Company, Seattle, Washington. Report Number D2-113072-2.

Farace, Richard V. and Hamish M. Russell. Beyond Bureaucracy--Message Diffusion as a Communication Audit Tool. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Flanagan, J. C. The Critical Incident Technique. Psychological Bulletin, 51:4, 1954, pp. 327-58.

Franc, Max B. Assessment of Attitude and Opinion Change Effects of the Communication Audit. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Greenbaum, Howard H. The Appraisal of Organizational Communication Systems. Paper presented at the International Communication Association, Atlanta, Georgia, April 19-22, 1972.

Haasl, David F. Advanced Concepts in Fault Tree Analysis. Paper presented at System Safety Symposium, University of Washington and the Boeing Company, Seattle, June, 1965.

Hawes, Leonard C. Information Overload and the Organization of 1984. Paper presented at the Western Speech Association Convention, Portland, Oregon, No. 23-25, 1970.

Helmer, Olaf. The Use of the Delphi Technique in Problems of Educational Innovations. P-3499. Santa Monica, California: RAND Corp., Dec. 1966.

Herzberg, Frederick. One More Time: How Do You Motivate Employees? Harvard Business Review, 46, Jan.-Feb. 1968, pp. 53-62.

Inoue, Michael S. Systems Research for Research Systems. Paper presented at the First Annual Meeting, Far West Region, Society for General Systems Research, Sept. 14-16, 1972.

Katz, Daniel and Robert L. Kahn. Communication: The Flow of Information. In Larry L. Barker and Robert J. Kibler, Eds., Speech Communication Behavior, Prentice-Hall, Inc., 1971, pp. 81-87.

San Leandro Unified School District in cooperation with the Bureau of Elementary and Secondary Education, California State Department of Education. Foreign Language Dropouts. Problems and Solutions. 1970.

Stephens, Kent G. A Fault Tree Approach to Analysis of Educational Systems as Demonstrated in Vocational Education. Unpublished doctoral dissertation, University of Washington, 1972.

Wilkinson, John. Retrospective Futurology. The Center Magazine. 5:6, November/December 1972, pp. 59-62.

Witkin, Belle Ruth. Management Information Systems. Applications to Educational Administration. Alameda County PACE Center, 1971. ERIC ED 057-608.

Witkin, Belle Ruth and Kent G. Stephens. Inservice Training in Using Fault Tree Analysis as a Technique for Evaluation and Management of Vocational Education Programs. Interim report, EPDA Project 01-700-EF-001-71, Alameda County School Department, Hayward, California, Sept. 1971.